## AMENDMENTS TO THE CLAIMS

Please add or amend the claims to read as follows, and cancel without prejudice or disclaimer
to resubmission in a divisional or continuation application claims indicated as cancelled:

1. – 39. (Cancelled)

40. (Currently amended) A method of identifying altered order critical data in a system for
conducting electronic commerce over a public data network, the system including a customer
computer to generate electronic orders for products selected by a customer, and to transmit
said orders over the public data network to a merchant computer for fulfilment by a merchant
in which orders are placed by a customer using a computer, wherein the method comprising
comprises the steps of:

        providing a validation server connected to the public data network;

        the validation server receiving transmitting an electronic order of the customer,
generated by the customer computer, over the public data network, wherein the electronic
order comprises order critical data that is protected from alteration and order data that is not
protected; from the customer computer to a validation server that validates order critical data
included in the order, the validation server executing the steps of:

        the validation server performing a verification of verifying said order critical data in
the electronic order; and

        the validation server generating an indication of the validity or invalidity otherwise of
the order critical data based upon said verification.

41. (Currently amended) The method of claim 40, wherein the indication of invalidity
whether the order critical data is valid or otherwise comprises an indication that the order
critical data has been altered in the event that the order critical data is invalid.

42. (Currently amended) The method of claim 40 further comprising the step of the validation
server transmitting the electronic order to at least one relevant merchant to be fulfilled for
fulfilment in the event that an indication of validity is generated the order critical data is
valid.

43. (Currently amended) The method of claim 40 further comprising ~~the step of~~ the validation server rejecting the electronic order in the event that an indication of invalidity is generated ~~the order critical data is invalid~~.

44. (Currently amended) The method of claim 40 further comprising the validation server executing ~~the steps of~~:

generating a report including information indicating whether or not said order critical data is valid; and

transmitting the report to one or more relevant merchants receiving the electronic order thus enabling said merchants to identify if order critical data in the electronic order is valid.

45. (Currently amended) The method of claim 40, wherein ~~further comprising the steps of~~:

~~providing a commerce server for serving product details;~~

~~the customer downloading~~ product details have been downloaded from [[the]] a commerce server to the customer computer over the public data network; and

~~generating~~ the electronic order has been generated by the customer computer using the product details downloaded from the commerce server.

46. (Currently amended) The method of claim 45, wherein said product details include the order critical data ~~is included in said product details~~ and comprising [[is]] digitally signing the order critical data ~~signed~~ with a secret key, and wherein:

the validation server receiving the electronic order further ~~the step of transmitting~~ comprises receiving ~~transmitting~~ the digital signature along with the electronic order; and

the validation server verifying the electronic order comprises ~~the step of the validation server~~ verifying that the digital signature corresponds with the order critical data.

47. (Currently amended) The method of claim 45, wherein the order critical data is duplicated in said product details, which comprise a first copy of the order critical data in unencrypted form and a second copy encrypted using a secret key, and wherein:

the validation server receiving the electronic order further comprises receiving ~~the step of transmitting includes transmitting~~ the encrypted copy of the order critical data along with the electronic order; and

the step of the validation server verifying the electronic order includes the validation server verifying that the encrypted data corresponds with the unencrypted order critical data in the electronic order.

48. (Currently amended) A validation server for identifying altered order critical data in a system for conducting electronic commerce over a public data network, the system including a customer computer to generate electronic orders for products selected by a customer, and to transmit said orders over the public data network to a merchant computer for fulfilment by a merchant in which orders are placed by a customer using a computer, the validation server comprising:

receiving means for receiving an electronic order of the customer transmitted over the public data network from the customer computer, wherein the electronic order comprises order critical data that is protected from alteration and order data that is not protected said electronic order including order critical data;

verifying means for verifying said order critical data in the electronic order; and

indicating means for generating an indication of whether the order critical data is valid or invalid based upon said verification of the verifying means otherwise, to enable altered order critical data to be identified.

49. (Currently amended) The validation server of claim 48 further including a report generating means for generating, on the basis of the indication generated by said indicating means, a report including information indicating whether or not said order critical data in the electronic order is valid or invalid.

50. (Previously presented) The validation server of claim 48, wherein the receiving means is adapted to receive a digital signature along with the electronic order, the digital signature being the result of digitally signing the order critical data with a secret key, and the verifying means comprises means for verifying that the digital signature corresponds with the order critical data.

51. (Previously presented) The validation server of claim 48, wherein the receiving means is adapted to receive duplicated order critical data comprising a first copy in unencrypted form and a second copy encrypted using a secret key, and the verifying means comprises means for

verifying that the encrypted data corresponds with the unencrypted order critical data in the electronic order.

52. (Currently amended) A method of operating a validation server, in a system for conducting electronic commerce over a public data network, the system comprising a customer computer to generate electronic orders for products selected by a customer, and to transmit said electronic orders over the public data network to a merchant computer for fulfilment by a merchant in which orders are placed by a customer using a computer, the method comprising the steps of:

receiving from the customer computer over the public data network an electronic order of the customer, wherein the electronic order comprises order critical data that is protected from alteration and order data that is not protected said electronic order including order critical data;

verifying said order critical data in the electronic order; and

generating an indication of the validity or invalidity otherwise of the order critical data.

53. (Currently amended) The method of claim 52, wherein the electronic order includes product details obtained from a commerce server, said product details being digitally signed with a secret key, and wherein the step of verifying the order critical data includes verifying that the digital signature corresponds with the order critical data.

54. (Currently amended) The method of claim 52, wherein the electronic order comprises product details obtained from a commerce server, said product details comprising a first copy of said order critical data in unencrypted form, and a second copy of said order critical data encrypted using a secret key, and wherein the step of verifying the order critical data comprises verifying that the encrypted data corresponds with the unencrypted order critical data in the electronic order.

55. (Currently amended) A method of a customer placing an order in a system for conducting electronic commerce over a public data network, the system including a customer computer to generate electronic orders for products selected by a customer, and to transmit said orders over the public data network to a merchant computer for fulfilment by a merchant whereby alterations to order critical data are identified, the method comprising the step of:

generating an electronic order, wherein the electronic order comprises order critical data that is protected from alteration and order data that is not protected including order critical data; and

transmitting the electronic order over the public data network to a validation server that verifies said order critical data, and generates an indication of the validity or invalidity otherwise of the order critical data.

56. (Currently amended) The method of claim 55, wherein the step of generating the electronic order comprises:

downloading relevant product details from a commerce server over the public data network; and

generating the electronic order using the product details downloaded from said commerce server.

57. (Currently amended) The method of claim 56, wherein the order critical data is included in said product details and is digitally signed with a secret key, and the step of transmitting the electronic order to the validation server comprises transmitting [[the]] a digital signature along with the electronic order, whereby the validation server verifies the order critical data by verifying that the digital signature corresponds with the order critical data.

58. (Currently amended) The method of claim 56, wherein the product details comprise a first copy of the order critical data in unencrypted form and a second copy of the order critical data encrypted using a secret key, and the step of transmitting the electronic order to the validation server comprises transmitting the encrypted copy of the order critical data along with the electronic order, whereby the validation server verifies the order critical data by verifying that the encrypted data corresponds with the unencrypted order critical data in the electronic order.

59. (Currently amended) A client-side software product for use in a customer computer in a system for conducting electronic commerce over a public data network where orders are placed by a customer using a computer, the client-side software product comprising[[:]] computer instruction code embodied on a tangible computer-readable medium that, when executed, causes the computer to:

generate ~~for generating~~ an electronic order of the customer, wherein the electronic order comprises order critical data that is protected from alteration and order data that is not protected ~~including order critical data~~; and

transmit ~~computer instruction code embodied on said computer-readable medium for effecting transmission of~~ the electronic order over the public data network from the customer computer to a validation server that verifies said order critical data and generates an indication of the validity or invalidity ~~otherwise~~ of the order critical data.